BY ORDER OF THE COMMANDER
AIR FORCE MATERIEL COMMAND

AIR FORCE INSTRUCTION 33-211

AIR FORCE MATERIEL COMMAND
Supplement 1

19 MARCH 2004

Communications and Information

COMMUNICATIONS SECURITY (COMSEC) USER REQUIREMENTS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: AFMC CSO/ITON
(Mr. Harry A. Wildermuth)
Supersedes AFI33-211_AFMCS1, 11Oct 02

Certified by: AFMC CSO/ITO
(Col. Kenneth A. Jeter)
Pages: 11
Distribution: F

AFI 33-211, 31Oct 2003, is supplemented as follows:

This supplement establishes command-unique Communications Security (COMSEC) management requirements. It defines policies and procedures applicable to COMSEC Managers (CMs), COMSEC Responsible Officers (CROs), COMSEC User Agencies (UAs), and contractors receiving COMSEC support from or managing AFMC-gained COMSEC accounts. Each CM is responsible for developing a supplement outlining local procedures for the CROs and UAs. Base supplements can add to, but not take away from the Air Force Instruction (AFI) and major command supplement. Provide a copy of each supplement to the AFMC COMSEC Office (HQ AFMC/CA624600). This supplement applies to all users who receive COMSEC material from AFMC COMSEC accounts, to include US Air Force Reserve (AFR) units. This publication applies to the Air National Guard (ANG) units when those units receive COMSEC materials from AFMC COMSEC accounts.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed.

3.1.5. Brief CROs on the usage of all new COMSEC aids issued to include effective dates and crypto periods. Will ensure each CRO is familiar with the usage and digraph for new aids issued to the CRO in order to prevent the use of superseded key. If the Controlling Authority provides status information, then the CM will ensure it is provided to the CRO at issue date and that the CRO comprehends the status information.

3.3.2. Ensure each applicable operation plan, order (or governing policy) directing the holding of COMSEC material, is reviewed annually to ensure holding requirements remain current.

3.3.3. Ensure each person granted access possesses a final clearance equal to or exceeding the classification level of the COMSEC material to be accessed.

3.3.4. Access lists will not be accepted as appointment letters for the position of CRO or alternate CRO. Access lists will be re-accomplished when adding new personnel. However, pen and ink revisions are permissible for the removal of names only. A name may be lined out with the initial of the CRO (or alternate) and the date accomplished noted next to the deleted name.

3.3.9. Each CRO will verify with the COMSEC account personnel the ALCs of any new COMSEC material being received (includes electronic key) prior to signing the hand receipt for the item(s).

3.3.14. If higher headquarters (MAJCOM level or higher) mandates a retention period for specific COMSEC records longer than specified in AFMAN 37-139, use that direction as your authority until AFMAN 37-139 is revised to reflect exceptions.

3.3.15. If the actions undertaken by the implementation of an EAP requires support by other agencies (or other sections within the organization) in order to meet the plan's objective then ensure coordination of the EAP is also made with those agencies.

3.3.17. Ensure these update reports follow the process established in Paragraph 61 of the basic instruction.

3.3.18. Ensure the CM provides instructions for non-duty hour notifications.

3.3.19. Accomplish semiannual training at a minimum of 5 months between training dates to ensure familiarity is achieved throughout the year. Semiannual training will not be accomplished in consecutive months (i.e. December-January) in order to just meet the requirements set by the basic instruction.

3.3.20. Must ensure they are fully aware of the crypto period and established purpose of all COMSEC aids issued to them. If specific handling instructions are provided by the Controlling Authority by message then the CRO will ensure these are provided by the COMSEC account when issued the material.

4. **Appointing COMSEC Responsible Officers (CRO).** The Facility Security Officer (FSO) or equivalent will be the authorizing official for Air Force contractor COMSEC User Agencies (UA) and activities.

4.1.3. The CM will ensure the security classification shown (facility clearance and level of safeguarding required) per the DD Form 254 matches or exceeds the level of the security classification of the COMSEC material requested by the contractor.

4.2. Reducing minimum grades by more than one grade requires concurrence from MAJCOM. Forward such requests through the CM to HQ AFMC/CA624600.

5. **Training.** Ensure initial training of new personnel is completed and documented prior to allowing them unescorted access or being allowed to handle COMSEC materials by themselves. Refresher training will be completed NLT 30 days from the date of when training was done the prior year.

5.1. (Added) Training is mandatory for all personnel listed on the access list.

5.2. (Added) Destroy training records when personnel no longer require access to COMSEC material and have been deleted from the access list.

6. **Operating Instructions (OI).** A contractor UA may title its operating instructions as Standard Practice Procedures or by any other corporate nomenclature as long as it meets the requirements set by the basic instruction and this supplement.

6.1. Coordinate the OI with the CM prior to establishing it.

6.3. Ensure these procedures are established in a separate OI for use when deployed, and it is marked or annotated to indicate clearly it is to be used only when on deployment. Maintain it separately from the in-garrison OI to avoid potential conflict and confusion in normal daily operations.

7. **Producing Communications Security Aids.** Ensure controlling authority approval is gained through the CM.

8. **Communications Security Forms.** CROs will ensure personnel tasked to deploy with COMSEC materials/aids are given sufficient and appropriate COMSEC forms for use in accomplishing their mission.

9.2. See Para **3.3.14.** of this supplement for additional disposition information. The CM may direct how these records are to be organized at each UA supported by the COMSEC account.

9.2.3. (Added) HQ AFMC/CA624600 may grant specific viewing access only to official agencies such as the Air Force Audit Agency and the Inspector General. They will not be permitted to reproduce or copy any document without prior approval from HQ AFMC/CA624600. These individuals will be under observation at all times by authorized COMSEC personnel. They will remain escorted in any area containing official records.

9.4. Retain a copy of all Wing COMSEC assessments conducted since the date of the last MAJCOM IAAP of the installation.

10.1.4. Contractors who receive CCI equipment via the CMCS will inventory the equipment by the AFCOMSEC Form 16.

10.1.4.1. (Added) CROs of other services (Navy, Army, Marines) who receive CCI equipment directly from their service's supply depot and not through the Air Force SBSS, will inventory their CCI equipment IAW with their respective services' direction. If their service directs CCI equipment to be inventoried as an ALC-1 item, the CRO may use the AFCOMSEC Form 16 as an inventory form and mark it "CCI Equipment Inventory." This specific information may ***not*** be included on, or combined with, the base COMSEC account AFCOMSEC Form 16. CCI equipment inventory will be *exempt* from Wing and MAJCOM COMSEC assessments.

11. **Status Information.** CROs are responsible for ensuring they have current status information from the CM on all COMSEC materials held requiring this information. This must always be checked and verified prior to receipting for the material. If the CRO is unsure as to the usage of the key, he or she must request additional guidance from the COMSEC account.

13.1. Ensure the requirements letter reflects COMSEC equipment and associated instructions that have been issued by the COMSEC account on a hand receipt (SF-153).

13.2. Contractor UAs without SBSS support from their sponsoring Air Force organization will order all COMSEC equipment via the COMSEC Material Control System (CMCS). Proof of accountability will require the CRO to exhibit the CA/CRL listing showing the equipment items to the CM. UAs with COMSEC equipment installed on aircraft are exempt from providing an inventory for viewing by the CM. The statement on the requirements letter will suffice for installed aircraft COMSEC equipment. In-transit units requiring support from AFMC COMSEC accounts are not required to show proof of COMSEC equipment on a CA/CRL listing. It is this has been accomplished by their home base COMSEC account.

14. **Over-The-Counter Service.** COMSEC account personnel will ***not*** serve the function of CRO or provide services as a CRO for any reason.

15. **Authorizing the Receipt and Transport of COMSEC Materials.** When the unit is deployable, ensure appointment letters cover potential deployments. Generic statements such as "Includes to, from and around deployed locations" on the appointment letter are permissible for personnel assigned to contingency units which can be tasked for short-notice deployments.

17. **Physical Security Requirements.** Ensure any construction modifications made to an area previously approved for the open storage of COMSEC material and aids are brought to the attention of your local security forces for possible recertification of the area. Contractor UAs will ensure this is brought to the attention of the FSO.

18.3. All personnel listed on the access list must receive COMSEC training. It will be documented on the AF Form 4168. CROs should take this into consideration when deciding if personnel (i.e. commanders and supervisors) who would infrequently require access and whose primary duties do not involve COMSEC operations should be placed on the list.

18.4. Contractor CROs will verify all clearance statuses through the FSO.

18.5. Access Control and Escort training is required of individuals who will be authorized to grant access to personnel not included on official access lists. At a minimum, this training must cover the procedures established in the OI to prevent unauthorized access to COMSEC materials and to prevent the viewing of COMSEC activities such as those identified under Para 18.2 of the basic instruction.

18.6. Contractors may use a company form in place of the AF Form 1109. This supplement supercedes any company guidance on the retention of visitor registers if such guidance directs the retention period to be less than 1 year from the date of the last visitor recorded.

19.4. Prepare a new SF-700 every time the combination is changed. Do not modify the form (i.e. laminating), so it can be routinely used as a template for recording the dates of combination changes.

19.4.1.6. (Added) Change the combination whenever a safe is brought into service.

19.4.1.7. (Added) Change the combination when the safe is being taken out of service or when no longer being used. Reset it to the standard combination of 50-25-50.

19.4.4. The CRO will adhere to and maintain a copy of TO 00-20F-2, *Inspection and Preventive Maintenance Procedures for Classified Containers* on file.

19.4.4.1. Record only the information required by TO 00-20F-2 on the AFTO Form 36. The form will be maintained within the container throughout the life of the container, even if it is transferred to another organization or taken out of service.

19.4.4.2. Check with the unit security manager to ensure the container markings are in accordance with the requirements of the installation or unit information security program. Contractor CROs will check with the FSO for guidance.

19.4.4.4. The procedures may be established as an addendum to the OI for ease in filing and reviews.

19.5. It is mandatory that authorized personnel are present whenever COMSEC materials are out of an approved GSA security container. Do not leave an area unattended while COMSEC materials are unsecured (or security containers containing COMSEC materials are open), depending on a cipher lock or a key locked door to prevent unauthorized access. This situation qualifies as a COMSEC incident, and the COMSEC manager must be notified.

20.3. Prepare the SF Form 701 for each month by annotating legibly or typing in block 1, “Opening handle pulled and verified” when security containers require a pull of an opening handle to access them. This will provide a reminder for personnel to test the handle by pulling to verify the container has indeed been secured and the locking mechanism is engaged. Use blue or black ink only in documenting daily security checks.

20.3.1. (Added) As part of the container check and verification process, personnel performing the end of day security check will also annotate on the SF Form 702, *Security Container Checklist* established for that container. Include the time and date the security container was checked as being secure in the appropriate block. Ensure all annotations are legible and in blue or black ink. Whether or not the security container was opened that day the check block will always be annotated as part of the daily security check. Facilities with 24-hour operations, and where the area is continuously manned, are exempt from this requirement as an entry made in the Master Station Log is sufficient.

20.3.2. (Added) Security containers with SF Form 702s which are stored in a larger GSA approved security container are exempt from having the security checks annotated on the SF 702 only when the larger container has not been opened for that day.

20.3.3. (Added) SF Form 702s will not be laminated or modified for continuous use, Prepare a new form for each month.

20.6. Contractor UAs may use a company form as a substitute for the SF Form 701, provided the requirements of both the basic instruction and this supplement are met.

30. **Routine Destruction Methods.** The CRO will consult the CM before using any destruction method listed in the basic instruction to ensure the methods, procedures, and devices used meet approved destruction requirements. If a destruction device is unavailable due to breakage then contact the CM for assistance in obtaining an alternate means to perform destruction.

31.1. The destruction official will be physically present and perform the destruction of the material listed in the destruction report.

31.2. The witnessing official will be present during the destruction process and view the destruction process in its entirety.

31.3. Destruction certificates will never be signed in advance of the actual destruction by either the destruction or witnessing official. Ensure all basic instruction and guidance is followed, before the destruction report is signed by either the destruction or witnessing official.

37.1. Prepare in memorandum format the listing of personnel authorized access to each combination and retain in the COMSEC folder.

39. **Recording Combinations.** Records of Top Secret COMSEC security container combinations are exempt from being entered or accounted for in the unit’s Top Secret Control Agency records by the unit Top Secret Control Officer.

41.4. (Added) The CRO will notify HQ AFMC/CA624600, through the CM, of any changes affecting the conditions by which the waiver was granted as soon as they are known.

44.3.2. Personnel newly assigned and placed on the COMSEC access list will be given initial EAP review and dry-run training prior to handling the COMSEC material or aids. Document the trainee's name, dates trained, and EAPs covered in this documentation.

44.3.3. Document All EAP reviews, dry-runs and actual events. For dry-runs and actual events, include the EAP used, date, location, persons participating, and a brief description of circumstances and results. Each participant will initial and date any documentation pertaining to reviews, dry-runs, and actual events. Records of actual events may be used to fulfill semiannual review and dry-run requirements. Personnel who are TDY, or on leave at the time the dry-runs are accomplished, will perform review and dry-run training upon their return to duty. To ensure uniformity for all COMSEC account UAs, the CM may require the use of a standard format for this documentation.

44.5. Coordinate with your unit commander to ensure he or she is aware and approves of the authority being granted in their name of personnel authorized to implement the Precautionary and Emergency Destruction EAPs.

Attachment 1

GLOSSARY OF REFERENCES, AND SUPPORTING INFORMATION

Abbreviations and Acronyms

CIK—Cryptographic Ignition Key

CM—COMSEC Manager

CMCS—COMSEC Material Control System

CRO—COMSEC Responsible Officer

DOD—Department of Defense

DTD—Data Transfer Device

EAP—Emergency Action Plan

FSO—Facility Security Officer

MAJCOM—AFMC COMSEC Office (CA624600)

NSI—Nuclear Surety Inspection

SPP—Standard Practice Procedure

DTD—Data Transfer Device

EAP—Emergency Action Plan

FSO—Facility Security Officer

NSI—Nuclear Surety Inspection

SPP—Standard Practice Procedure

Attachment 9 (Added)

TRANSPORTATION OF COMSEC MATERIAL

A9.1. (Added) PREPARATION FOR TRANSPORTATION . When preparing to transport classified COMSEC material, follow the requirements of AFI 31-401 and DOD 5200.1-R as appropriate. Always check with the CM prior to transporting COMSEC materials for any reasons other than the normal transport of the COMSEC monthly issue received from the COMSEC account.

A9.1.1. (Added) Double-wrap or otherwise encase all classified COMSEC material in two opaque containers and security seal prior to transportation. Use strong and durable packing materials that provide protection while in transit, prevents items from breaking through the container, and facilitates the detection of any tampering with the container. Do not indicate on the outer wrapper that the package contains classified material or keying material.

A9.1.1.1. (Added) COMSEC items may be sealed in individual wrappers, envelopes, or protective packaging that allows for the identification of the item or publication for inventory purposes without having to open it. These wrappers, envelopes, or protective packaging do not qualify as the inner wrapper when packaging COMSEC material for shipment.

A9.1.2. (Added) Appropriately wrap unclassified COMSEC material (other than keying material), in a way that tampering or penetration of the wrapping can be detected. Ensure the wrapping protects the material from damage.

A9.1.3. (Added) When material is carried, a briefcase, pouch, or box is an appropriate outer wrapper.

A9.2. (Added) Transportation of Keying Material . Do not transport operational keying material in the same container with its associated equipment. Unclassified maintenance key approved for usage with the associated equipment may be shipped in the same container.

A9.2.1. (Added) Check with the CM prior to shipping or couriering COMSEC keying material anywhere outside the installation. Units which routinely issue COMSEC materials to aircrews in support of flying operations are exempt from having to notify the CM.

A9.3. (Added) Transportation of COMSEC Equipment .

A9.3.1. (Added) CCI equipment will be transported according to the requirements established in AFI 33-275, *Controlled Cryptograph Items (CCI)*. Contractor UAs not supported by the SBSS, who have received their COMSEC equipment via hand-receipt, will transport their CCI equipment only by CM direction.

A9.3.2. (Added) Classified COMSEC equipment received through the CMCS will be transported only by direction of the CM. Units with a requirement for shipping or couriering classified COMSEC equipment will contact the CM for guidance.

A9.4. (Added) Methods of Conveyance .

A9.4.1. (Added) Use of private vehicles or corporate-owned vehicles are permitted to carry COMSEC materials provided the recipient organization is aware of the itinerary and is given an estimated time of arrival so that appropriate steps may be taken if the courier does not arrive on time.

A9.4.1.1. (Added) Units transporting COMSEC material or aids from the COMSEC account as part of the monthly issue should make someone in their office aware they will be picking up the monthly issue and estimated time of return.

A9.4.2. (Added) Use of commercial airlines for transporting COMSEC materials will only be accomplished by direction of the CM.

A9.4.3. (Added) The electronic transfer of keying material is prohibited and will only be accomplished through the CM.

A9.5. (Added) Actions taken after the delivery of transported COMSEC items will consist at a minimum, inspection of the packages for evidence of tampering, penetration or damage. If these are discovered then notify the CM immediately.

Attachment 10 (Added)

COMSEC RECORDS DISPOSITION INSTRUCTIONS

A10.1. (Added) Use the following guide for maintaining and disposing of COMSEC records:

Table A10.1. (Added) Guide For Disposing Of COMSEC Records.

Form/Document	Instructions
AFCOMSEC Form 1, **COMSEC Users Receipt/Destruction Certificate**	Transfer the DRC to the COMSEC account when accomplished.
AFCOMSEC Form 21, **Disposition Record for KI-1B/C Keytapes**	Transfer the DRC to the COMSEC account when accomplished.
AFCOMSEC Form 22A, **Disposition Record for Single Copy Keytapes**	Transfer the DRC to the COMSEC account when accomplished.
AFCOMSEC Form 22B, **Disposition Record for Multi-copy Keytapes**	Transfer the DRC to the COMSEC account when accomplished.
AFCOMSEC Form 9, **Cryptographic Access Certificate**	Destroy 90 days after date of withdrawal, unless withdrawn for cause. In that case, destroy when all inquiries/investigations are completed
AFCOMSEC Form 16, **COMSEC Account Daily Shift Inventory**	Maintain current plus last 6 months.
AF Form 4168, **COMSEC Responsible Officer and User Training Checklist**	Maintain current documentation only for personnel on the access list
AF Form 1109, **Visitor Register Log**	Maintain 12 months from date of last visitor signed in
AFTO Form 36, **Maintenance Record for Security Type Equipment**	Permanent. Keep with safe.
SF 700, **Security Container Information**	Destroy when superceded.
SF 701, **Activity Security Checklist**	Maintain current only.
SF 702, **Security Container Check Sheet**	Maintain current only.
Local Destruction Reports (SF 153, **COMSEC Material Report**)	Destroy 3 years after date of material destruction.
All Waivers	Maintain original and all renewals until the waiver is terminated.
Operating Instructions (with coordination)	Maintain current only
EAPs (with coordination)	Maintain current only.
EAP Dry Run Records	Maintain and hold till next command COMSEC assessment
Information Assurance Assessment Reports and Follow-ups (MAJCOM and wing)	Destroy after next command COMSEC assessment.
COMSEC Incident Reports and Follow-ups	Destroy 1 year after date report is closed.

Form/Document	Instructions
Facility Access Lists	Maintain current only
Functional Review, Visitor, and COMSEC Manager Access Lists	Maintain current only
Technical Countermeasures Surveys	Maintain current only
Two-Person Integrity Appointments	Maintain current only
Primary and Alternate CRO Appointments	Maintain current only
Courier Letters	Maintain current only
Hand Receipts (SF 153)	Destroy when all material listed on any given hand receipt is destroyed or transferred

KENNETH H. PERCELL, Director
Information Technology